IN THE CLAIMS

Please amend the claims as follows:

Claims 1-4 (Canceled).

Claim 5 (Withdrawn): A revoke control data generating device comprising:

a device key matrix storage unit configured to store a device key matrix in which device keys are arranged in a two dimensional manner;

a device key generating device configured to select one of the device keys in each one dimensional array of the device key matrix according to each numeral of a device ID;

an encrypting unit configured to encrypt the selected device keys by a master key; and

a revoke control data generating unit configured to generate revoke control data including an output of said encrypting unit and a path function indicating a path of the device ID to be revoked in a tree formed of all possible combinations of the numerals forming a device ID.

Claim 6 (Withdrawn): The revoke control generating device according to claim 5, wherein said device key generating device selects one of device keys in each row of the key matrix according to each numeral of the device ID.

Claim 7 (Withdrawn): A content utilizing device comprising:

a device information storing unit configured to store a device information including an arrangement of device keys and a device ID;

a key decrypting unit configured to receive revoke control data including encrypted data keys which are encrypted by a master key and decrypt the encrypted data keys to obtain the master key; and

a content decrypting unit configured to receive content data which is encrypted by the data keys and decrypt the encrypted content data using the master key, wherein if the device information is included in the received revoke control data, the content utilizing device is revoked such that the key decrypting unit does not obtain the master key.

Claim 8 (Withdrawn): The content utilizing device according to claim 7, wherein said revoke control data comprises a path function indicating a path of the device ID in a tree formed of all possible combinations of the numerals forming the device ID.

Claims 9-10 (Canceled).

Claim 11 (Withdrawn): A device information generating method comprising:

selecting one of device keys in a device key matrix in which device keys are arranged in a two dimensional manner in each one dimensional array of the device key matrix according to each numeral of a device ID; and

calculating a path function value based on the selected device keys, the path function indicating a path of the device ID in a tree formed of all possible combinations of the numerals forming the device ID,

wherein path function value and the device ID are the device information.

Claim 12 (Withdrawn): The device information generating method according to claim 11, wherein one of the device keys in each row of the key matrix is selected according to each numeral of the device ID.

Claim 13 (Withdrawn): A revoke control data generating method comprising:

selecting one of device keys in a device key matrix in which device keys are arranged in a two dimensional manner in each one dimensional array of the device key matrix according to each numeral of a device ID;

encrypting the selected device keys by a master key; and

generating revoke control data including the encrypted-selected device keys and a path function indicating a path of the device ID to be revoked in a tree formed of all possible combinations of the numerals forming a device ID.

Claim 14 (Withdrawn): The revoke control generating method according to claim 13, wherein one of the device keys in each row of the key matrix is selected according to each numeral of the device ID.

Claim 15 (Withdrawn): A content utilizing method comprising:

receiving revoke control data including encrypted data keys which are encrypted by a master key and decrypting the encrypted data keys to obtain the master key; and

receiving content data which is encrypted by data keys stored in a content utilizing device and decrypting the encrypted content data using the master key, wherein if device information formed of a device information including an arrangement of the device keys and a device ID is included in the received revoke control data, the content utilizing device is revoked such that the encrypted data keys are not decrypted.

Claim 16 (Withdrawn): The content utilizing method according to claim 15, wherein said revoke control data comprises a path function indicating a path of the device ID in a tree formed of all possible combinations of the numerals forming the device ID.

Claim 17 (Withdrawn): An article of manufacture comprising a computer usable medium having computer readable program code means embodied therein, the computer readable program code means comprising:

computer readable program code means for causing a computer to select one of device keys in a device key matrix in which device keys are arranged in a two dimensional manner in each one dimensional array of the device key matrix according to each numeral of a device ID;

computer readable program code means for causing a computer to encrypt the selected device keys by a master key; and

computer readable program code means for causing a computer to generate revoke control data including the encrypted-selected device keys and a path function indicating a path of the device ID to be revoked in a tree formed of all possible combinations of the numerals forming a device ID.

Claim 18 (New): A revoke control method for revoking at least one of a plurality of content utilizing devices, each of the content utilizing devices being assigned a device ID and assigned a set of device keys according to the device ID, the device ID being formed of numerals each indicating a position of each of the device keys of the set in each one dimensional array of a device key matrix in which device keys are arranged in a two dimensional manner, and the device ID indicating a path in a plurality of trees that are formed of all possible combinations of device keys in the device key matrix, the method comprising:

preparing the device key matrix;

inputting a revoke target path, which is a path to be revoked in the trees and formed of numerals each indicating a position of a device key in each one dimensional array of the device key matrix;

calculating a boundary set of paths except for the revoke target path in the trees, each of the paths of the boundary set being formed of one or more numerals each indicating a position of a device key in each one dimensional array of the device key matrix;

calculating a path function value corresponding to each of the paths of the boundary set based on each device key indicated by each numeral of the each of the paths of the boundary set, to obtain a plurality of path function values corresponding to the paths of the boundary set;

encrypting a master key by using each of the path function values, to obtain a plurality of encrypted data items corresponding to the paths of the boundary set;

generating revoke control data including the encrypted data items; and

outputting the revoke control data to the each of the content utilizing devices,

each content utilizing device whose device ID indicates one of the boundary set of paths configured to decrypt one of the encrypted data items by using a path function value calculated based on one or more device keys of the set assigned to the each content utilizing device.

Claim 19 (New): The revoke control method according to claim 18, wherein the each of the content utilizing devices includes a memory to store the device ID assigned to the each of the content utilizing devices and a set of path function values each calculated based on one or more device keys of the set assigned to the each of the content utilizing devices; and

the each content utilizing device whose device ID indicates one of the boundary set of paths configured to decrypt one of the encrypted data items by using one of the path function values stored in the memory.

Claim 20 (New): The revoke control method according to claim 18, wherein the each of the content utilizing devices includes a memory to store the device ID and the set of device keys assigned to the each of the content utilizing devices; and

the each content utilizing device whose device ID indicates one of the boundary set of paths configured to calculate the path function value based on one or more device keys of the set stored in the memory, and decrypt one of the encrypted data items by using the path function value calculated.

Claim 21 (New): The revoke control method according to claim 20, wherein the each content utilizing device whose device ID indicates one of the boundary set of paths configured to calculate the path function value based on the one or more device keys of the set which are on a partial path included in the path indicated by the device ID of the each content utilizing device.

Claim 22 (New): The revoke control method according to claim 18, wherein each numeral of the device ID corresponds to a row in each column of the device key matrix, each numeral of the revoke target path corresponds to a row in each column of the device key matrix, and each numeral of the each of the paths of the boundary set corresponds to a row in each column of the device key matrix.

Claim 23 (New): A content utilizing device assigned a device ID and assigned a set of device keys according to the device ID, the device ID being formed of numerals each indicating a position of each of the device keys of the set in each one dimensional array of a device key matrix in which device keys are arranged in a two dimensional manner, and the device ID indicating a path in a plurality of trees that are formed of all possible combinations of device keys in the device key matrix, the content utilizing device comprising:

a memory to store the device ID and a plurality of path function values each calculated based on one or more device keys of the set which are on a partial path included in the path indicated by the device ID;

an input unit configured to input revoke control data generated by a revoke control data generating device configured to:

(a) calculate a boundary set of paths except for a revoke target path in the trees which is a path to be revoked in the trees and is formed of numerals each indicating a position of a device key in each one dimensional array of the device key matrix, each of the paths of the boundary set being formed of one or more numerals each indicating a position of a device key in each one dimensional array of the device key matrix;

(b) calculate a path function value corresponding to each of the paths of the boundary set based on each device key indicated by each numeral of the each of the paths of the boundary set, to obtain a plurality of path function values corresponding to the paths of the boundary set;

(c) encrypt a master key by each of the path function values, to obtain a plurality of encrypted data items corresponding to the paths of the boundary set; and

(d) generate the revoke control data including the encrypted data items; and

a decryption unit configured to decrypt one of the encrypted data items by using one of the path function values stored in the memory when the path indicated by the device ID stored in the memory is included in the boundary set of paths.

Claim 24 (New): The content utilizing device according to claim 23, wherein each numeral of the device ID corresponds to a row in each column of the device key matrix, each numeral of the revoke target path corresponds to a row in each column of the device key matrix, and each numeral of the each of the paths of the boundary set corresponds to a row in each column of the device key matrix.

Claim 25 (New): A revoke control data generating device generating a revoke control data for revoking at least one of a plurality of content utilizing devices, each of the content utilizing devices being assigned a device ID and assigned a set of device keys according to the device ID, the device ID being formed of numerals each indicating a position of each of the device keys of the set in each one dimensional array of a device key matrix in which device keys are arranged in a two dimensional manner, and the device ID indicating a path in a plurality of trees that are formed of all possible combinations of device keys in the device key matrix, the revoke control data generating device comprising:

a memory to store the device key matrix;

an input unit configured to input a revoke target path which is a path to be revoked in the trees and is formed of numerals each indicating a position of a device key in each one dimensional array of the device key matrix;

a first calculation unit configured to calculate a boundary set of paths except for the revoke target path in the trees, each of the paths of the boundary set being formed of one or

more numerals each indicating a position of a device key in each one dimensional array of the device key matrix;

a second calculation unit configured to calculate a path function value corresponding to each of the paths of the boundary set based on each device key indicated by each numeral of the each of the paths of the boundary set, to obtain a plurality of path function values corresponding to the paths of the boundary set;

an encryption unit configured to encrypt a master key by using each of the path function values, to obtain a plurality of encrypted data items corresponding to the paths of the boundary set; and

a generation unit configured to generate the revoke control data including the encrypted data items.